BỘ BƯU CHÍNH VIỄN THÔNG

Số: 03/2007/CT-BBCVT

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà nội, ngày 23 tháng 02 năm 2007

CHỈ THỊ

V/v: Tăng cường đảm bảo an ninh thông tin trên mạng Internet

Trong thời gian vừa qua, tình hình an ninh thông tin trên Internet diễn biến phức tạp. Nhiều trang thông tin điện tử bị tấn công, bị thay đổi nội dung. Không ít trang thông tin của Việt Nam sử dụng tên miền quốc tế bị mất hoặc bị chuyển hướng, vi rút, thư rác phát tán mạnh. Một số mạng mang địa chỉ IP của Việt Nam do phát tán vi rút hay thư rác đã bị cấm kết nối quốc tế, cấm giao dịch điện tử… Theo khảo sát sơ bộ có tới 80% các trang tin điện tử còn nhiều sơ hở trong đảm bảo an ninh thông tin, nhiều hệ thống thông tin còn có khiếm khuyết chưa được cập nhật và quan tâm đúng mức nên đã gây ra những sự cố đáng tiếc ảnh hưởng tới các dịch vụ hành chính điện tử, thương mại điện tử và các hình thức ứng dụng công nghệ thông tin khác. Nhận thức về nguy cơ mất an ninh thông tin và thiệt hại khi xảy ra sự cố mạng của nhiều cơ quan, tổ chức và doanh nghiệp còn nhiều hạn chế.

Để tăng cường đảm bảo an ninh thông tin trên Internet, hạn chế hậu quả xấu có thể xảy ra đối với các trang thông tin điện tử nhất là của các cơ quan nhà nước, tổ chức và doanh nghiệp trên toàn quốc, Bộ trưởng Bộ Bưu chính, Viễn thông yêu cầu các cơ quan, tổ chức và doanh nghiệp:

1. Nghiêm chỉnh chấp hành pháp luật về bưu chính, viễn thông và Internet, Luật công nghệ thông tin, Luật giao dịch điện tử; có trách nhiệm đảm bảo an ninh thông tin trong hoạt động Internet; thực hiện các yêu cầu về đảm bảo an ninh thông tin của Bộ Bưu chính Viễn thông, Bộ Công an và các cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.

2. Các cơ quan, tổ chức tham gia hoạt động trên mạng Internet phải:

a) Rà soát, kiểm tra, đánh giá các hệ thống thiết bị phục vụ việc lưu trữ, cung cấp và truyền tải thông tin; đánh giá hiện trạng các hệ thống bảo vệ và các biện pháp đảm bảo an ninh thông tin. Ưu tiên sử dụng các kết nối trong nước, tên miền ".vn" để đảm bảo an toàn cho trang thông tin điện tử.

b) Xây dựng quy trình và quy chế đảm bảo an ninh thông tin cho các hệ thống thông tin, tham khảo các chuẩn quản lý an toàn TCVN 7562, ISO 27001. Đảm bảo khả năng truy vết và khôi phục thông tin trong trường hợp có sự cố.

c) Thường xuyên phối hợp với cơ quan hữu quan và các tổ chức cung cấp dịch vụ an toàn mạng cập nhật các biện pháp đảm bảo an ninh thông tin mới nhất.

3. Các doanh nghiệp viễn thông và internet tăng cường kiểm tra, giám sát chặt chẽ các trang thiết bị thuộc quyền quản lý; không được lợi dụng hoặc để người khác lợi dụng gây mất trật tự an toàn xã hội; các hệ thống thiết bị, các phần mềm đưa vào sử dụng trên mạng Internet tuân thủ theo quy định tại mục 2b.

4. Các doanh nghiệp cung cấp dịch vụ giá trị gia tăng trên Internet *(hosting, mail, FTP…)* phải có các biện pháp đảm bảo an ninh thông tin.

5. Các đơn vị, cá nhân cần thông báo sự cố và nguy cơ mất an toàn thông tin về các sở Bưu chính Viễn thông ở địa phương và về Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) trực thuộc Bộ Bưu chính Viễn thông.

6. Các tổ chức, doanh nghiệp tham gia hoạt động trên mạng Internet hoặc cung cấp dịch vụ an toàn an ninh mạng phải nghiêm túc thực hiện sự điều phối của Trung tâm VNCERT trong hoạt động ứng cứu sự cố mạng Internet ở Việt Nam, hợp tác với Trung tâm VNCERT trong việc kiểm tra đánh giá năng lực đảm bảo an toàn mạng trong đơn vị mình khi có dấu hiệu hay nguy cơ mất an toàn mạng.

7. Các đơn vị trực thuộc Bộ Bộ Bưu chính Viễn thông theo chức năng và nhiệm vụ có trách nhiệm cử cán bộ có năng lực phối hợp với VNCERT trong việc đấu tranh phòng chống tấn công trên mạng; tiến hành huấn luyện nghiệp vụ, đào tạo cập nhật về an ninh thông tin cho các cơ quan, tổ chức và cá nhân có nhu cầu.

8. Trung tâm VNCERT nhanh chóng triển khai hệ thống thu thập thông tin và tư vấn qua mạng Internet; chủ trì phối hợp với các cơ quan liên quan xây dựng và triển khai kế hoạch đào tạo bồi dưỡng nghiệp vụ an toàn thông tin đáp ứng nhu cầu thực tiễn của các cơ quan, tổ chức và doanh nghiệp; tăng cường công tác tuyên truyền nâng cao nhận thức của cộng đồng về trách nhiệm đảm bảo an ninh thông tin trong các hoạt động viễn thông và Internet.

9. Trung tâm Internet Việt Nam (VNNIC) có trách nhiệm tăng cường quản lý tên miền quốc gia ".vn", địa chỉ IP theo quy định; tăng cường bảo đảm an toàn an ninh cho hệ thống máy chủ tên miền quốc gia; phối hợp với các đơn vị chức năng cung cấp các thông tin về tên miền địa chỉ theo yêu cầu.

10. Các Sở Bưu chính Viễn thông tăng cường công tác quản lý nhà nước về đảm bảo an ninh thông tin trong hoạt động Internet theo thẩm quyền được giao; hướng dẫn các doanh nghiệp viễn thông và internet, các đại lý internet trên địa bàn thực hiện nghiêm chỉnh các quy định của pháp luật về Bưu chính Viễn thông và internet; đẩy mạnh công tác thanh tra, kiểm tra và xử lý kịp thời, kiên quyết các vi phạm về an ninh thông tin; kiện toàn tổ chức, nâng cao năng lực cán bộ đáp ứng yêu cầu thực hiện.

Thủ trưởng các cơ quan, đơn vị trực thuộc Bộ, Sở Bưu chính Viễn thông, cơ quan, tổ chức tham gia hoạt động trên mạng Internet có trách nhiệm tổ chức, triển khai thực hiện Chỉ thị này và gửi báo cáo kết quả thực hiện về Bộ Bưu chính, Viễn thông (Trung tâm VNCERT) vào cuối Quý I/2007; trong quá trình thực hiện, nếu có vướng mắc phát sinh, báo cáo Bộ Bưu chính, Viễn thông xem xét giải quyết.

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam có trách nhiệm kiểm tra, đôn đốc việc thực hiện Chỉ thị này và báo cáo Bộ trưởng.

BỘ TRƯỞNG

(Đã ký)

Đỗ Trung Tá